Cybersecurity

2022/2023

Questions and exercises

Questions:

1) List and briefly define categories of security services.
2) What is the difference between passive and active security threats?
3) What is the difference between a block cipher and a stream cipher?
4) List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
5) What is the difference between an unconditionally secure cipher and a computationally secure cipher?
6) Briefly define the monoalphabetic cipher.
7) What is the avalanche effect for an encryption algorithm?
8) Which of the following block cipher modes of operation ECB, CBC, OFB, CFB, CTR, use only the encryption function for both encryption and decryption?
9) What characteristics are needed in a secure hash function?
10) List possible usages of hash function.
11) What is a message authentication code?
12) Consider a hash function H(.) that iteratively processes the input message in blocks of size M using a compression function C (an example could SHA1 that uses a C function of size 512 bits). Show the scheme of HMAC as function of H, and evaluate the number of C passes (number of calls of the function C) required to calculate the HMAC of a message m with length N.M.
13) What is the meaning of the expression a≡b (mod n)?
14) How it is defined the multiplicative inverse of an integer modulo n?
15) What is Euler’s totient function?
16) What is the discrete logarithm?
17) Describe RSA encryption algorithm.
18) Describe Diffie-Hellman key exchange.
19) Show how RSA digital signature and verification work.
20) Show possible challenge-response identification schemes based on symmetric cipher, asymmetric cipher, hash function, MAC function, or digital signature.
21) Show different ways in which secret keys can be established between two parties.
22) What is the difference between a short-term key (session key) and a long-term key?
23) What is a key distribution center? Describe a possible key distribution scheme that uses a KDC.
24) Why Diffie-Hellman key exchange is vulnerable to Man-in-the-middle attack? Show an example of successful MITM attack to the DH.
25) Describe how the Diffie-Hellman key exchange can be generalized for group key exchange.
26) What is a digital certificate?
27) What is a chain of certificates?

28) What information is included in a X.509 certificate?

29) What is a X.509 Certification Revocation List (CRL)?

30) Which are the security services provided by IPSec ESP?

31) Which are the security services provided by TLS?

32) Which certificate is usually involved in a TLS handshake between a client an a server?

33) Describe a possible scheme for a high-latency anonymity system based on multiple mixes (mix network).

34) What is an Onion Routing anonymity system?

35) What is the different between a sniffing attack and a Man-In-The-Middle attack?

36) Describe what a spoofing attack is.

37) Describe what a DoD attack is.

38) Differences between a network scanner and a vulnerability scanner.

39) Describe what a buffer overflow attack is.

40) What is a SQL injection attack?

41) What is a packet filtering firewall?

42) What is a an Intrusion Detection System?

Exercises:

1) Let us consider a simple monoalphabetic shift cipher (Caesar's Cipher), with an alphabet of di N characters (with N= 26), with a secret key K=4 (the shift). Do encrypt the text "SECRET".

2) Consider a monoalphabetic substitution cipher, that maps a plaintext character *M* into the cipher character *C,* defined as follows:

$C = E_k(M) = a M + b \bmod 26$

where *M* is any character of the alphabet {'a','b', 'c', .. ,'z'}, and a and b are two integer parameters that form the secret key *K* = <a,b>

By using such a cipher, a ciphertext has been generated starting from an English plaintext. By analyzing the ciphertext it results that the most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'.

Try to break this code, by knowing that the two most frequent letters in English are 'e' and 't'.

(Hints: $x \bmod n = y \Rightarrow \exists\, h : x = y + hn$. The equation $15x \bmod 26 = 19$ has the solution $x = 3$).

3) Starting from a block cipher $E_K(\cdot)$ with block size *q*, please show the scheme for the CBC (Cipher Block Chaining) encryption of a message *m* with length *L*>*q* (for simplicity, let's consider *L*=*n q*).

4) Suppose to have an API implementing a block cipher *E* in CBC mode, with block size *q*. The same block cipher in CBC mode has been used to encrypt a message *m* with length *pq* using a key *K* of size *n* bits. Evaluate the complexity of a brute force attack against the secret key *K*, by supposing to know both the plaintext *m* and the ciphertext *c*. In each attempt, the entire message is processed. Indicate the complexity in terms of the number of block encryptions (using the function *E*), as function of *n*, *p,* and *q*.

5) Let us consider a symmetric block cipher $E_k(\cdot)$ with size 4 bit. By supposing that, given a secret key *K*, the encryption table of $E_k(\cdot)$ corresponds to the table at the right side, do encrypt in CBC mode with IV=0000 the following plaintext message:

m= `1100 1010 0010 1101`

plaintext	***ciphertext***
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010

1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

6) Let us consider the following plaintext message:

m = `1100 0000 1100 0000`

encrypted by means of the same symmetric encryption algorithm $E_k(\cdot)$ with block size 4bit and secret key K of the previous exercise (same encryption/substitution table) in OFB mode with IV=0001, resulting the following ciphertext:

c = `1000 0010 0001 1001 (IV=0001)`

Show how it is possible to modify the ciphertext c in such a way that by decrypting it you obtain the following plaintext:

m'= `1100 0000 1001 0000`

7) Let us consider a message *m=M1||M2||M3||M4*, and suppose to encrypt it by means of a block cipher $E_K()$ in CBC mode (the block size of $E_K()$ is equal to the size of the blocks *Mi*), with *iv=IV0*, obtaining the ciphertext *c= C1||C2||C3||C4*. If an attacker modifies the ciphertext by rearranging the component blocks obtaining the new ciphertext c'= *C1||C3||C2||C4*, which will be the corresponding plaintext message *m'=M'1||M'2||M'3||M'4* obtained by "erroneously" decrypting the ciphertext *c'*? Show the blocks *M'i* as function of *Mj* and *Cj* with *j=1..4*.

8) Realize a symmetric encryption scheme for encrypting messages *m* with any length, based on a block cipher $E_K()$ (e.g. AES), without obtaining avalanche effect, in such a way that if you change one bit of the ciphertext, only one bit of the plaintext will change when decrypting the ciphertext (hint: use the XOR operator).

9) Consider the following three padding algorithms for extending the length of a message to a multiple of N bytes (e.g. N=32). Which of the three algorithms are suitable for using with a block cipher with block size N bytes? Why?

Padding1: append to the message random bytes until the total length (in bytes) becomes a multiple of N.

Padding2: append to the message random bytes until the total length (in bytes) becomes a multiple on N – 1; append one byte encoding the number of padding bytes that have been added.

Padding3: append to the message a bit '1', then append as many bits '0' as needed to reach a multiple of N bytes.

10) Starting from a hash function H() and a symmetric key K_{AB} shared between two entities A e B:

i) show a possible authentication scheme between A (supplicant) and B (authenticator);

ii) show how it is possible to send a message *m* from A to B providing data authentication and integrity protection;

iii) create an encryption function (and the corresponding decryption function) that can be used for sending a message *m* encrypted from A to B.

11) Find the multiplicative inverse of each nonzero element in $\mathbb{Z}_7$.

12) Find all nonzero elements in Z_{21} that are relatively prime with 21.

13) By using the Euclid's algorithm, find the greatest common divisor gcd(,) of:

a) 36, 15

b) 47, 20

c) 43, 35

14) Prove the following: If *p* and *q* are prime, then $\Phi(pq) = (p-1)(q-1)$.

(Hint: What numbers have a factor in common with *pq*?)

15) Create a pair of public/private RSA keys, using as *p* and *q* primes the values p=3, q=11. With such keys, do encrypt the plaintext message m=2.

16) With the following values p=7, q=11 and e=13. Create a pair of public/private RSA keys KU=<e,n> and KR=<d,n> (Use the Euclid's algorithm for finding the value d). With such keys, do decrypt the ciphertext message c=2.

17) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$.What is the plaintext M?

18) In an RSA system, the public key of a given user is $e = 31$, $n = 901$.What is the private key of this user? (*Hint:* First use trial-and-error to determine *p* and *q*; then use the extended Euclidean algorithm to find d)

19) Show an example of shared key exchange between A and B based on Diffie-Hellman scheme, using the generator g=2 and the prime p=11.

20) Show that 2 is a primitive root of 11.

21) Users A and B use the Diffie-Hellman key exchange technique with a common prime p=71 and a primitive root g=7.
i. If user A has private key x_A=5, what is A's public key y_A?
ii. If user B has private key x_B=12, what is B's public key y_B?
iii. What is the shared secret key K_{AB}?

22) Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing ONLY the data confidentiality. For message encryption you should use a symmetric encryption algorithm (since it is faster than asymmetric algorithm). By supposing that A and B share only their public RSA keys KU_A e KU_B (KR_A and KR_B are the private keys), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes.

23) Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing ONLY data authentication/integrity. By supposing that A and B share only a secret key K_{AB} and a hash algorithm H(), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes.

24) Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing both confidentiality and data authentication/integrity. For message encryption you should use a symmetric encryption algorithm (since it is faster than asymmetric algorithm). By supposing that A and B share only their public RSA keys KU_A e KU_B (KR_A and KR_B are the private keys), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes. A and B share the following algorithms: RSA, AES, SHA1.

25) Let us suppose that you want to securely send a message *m* from A to two recipients B and C, by guaranteeing both confidentiality (through symmetric encryption with algorithm $E_k()$) and data authentication/integrity (through digital signature). Let us suppose that A, B and C have their own private RSA keys, K^-_A, K^-_B e K^-_C, and that they share all their public keys K^+_A, K^+_B e K^+_C.
Please show which functions could be executed by A (sender), and the resulting message *x* that is actually sent from A to B and C.

26) Show a possible secure authentication scheme between Alice (supplicant) and Bob (authenticator), by supposing that Alice and Bob share their public RSA keys KU_A and KU_B (KR_A and KR_B are the corresponding private keys).

27) Show a possible mutual authentication scheme between Alice and Bob, based on the use of an hash function H(˙) and a shared secret K_{AB}.

28) Show a possible key transport scheme between two entities A and B, based on asymmetric encryption (public key cryptography), without the use of a KDC.

29) Show an example of authenticated DH exchange that holds out against MITM attack.

30) Let us consider an entity A that holds the following digital certificates: cert_{CA3}(A), cert_{CA2}(CA3), cert_{CA1}(CA2), and cert_{CA1}(CA1) (where cert_{Y}(X) refers to the certificate of X signed by Y). Indicate what A should send to B in order to let A and B start a secure communication, under the following different hypotheses:

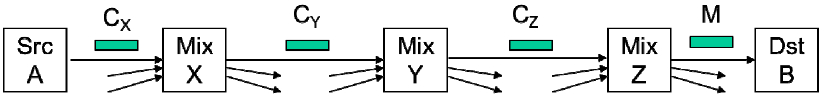
B owns:	A should send to B:
cert_{CA1}(CA1)	
cert_{CA3}(A)	
cert_{CA1}(CA2)	
cert_{CA1}(CA1), cert_{CA3}(A)	

31) If A holds cert_{B}(A) and cert_{C}(B) (where cert_{Y}(X) refers to the certificate of X signed by Y), while D holds cert_{E}(D), please indicate:

a. what should A hold in order to authenticate D? Show a possible authentication scheme.

b. what should D hold in order to authenticate A? Show a possible authentication scheme.

32) Let us consider an anonymizing network formed by high-latency anonymizing *Mix* nodes. Let us consider the case in which a node *A* wants to send a message *m* to a node *B* by means of three intermediate *Mix* nodes *X*, *Y*, and *Z*. Assume that K^{+}_{i} and K^{-}_{i} are respectively the public and private keys of node *i* (*i*=*x*,*y*,*z*).
Indicate the format of the message C_X composed by *A* and sent to the first node *X*.



33) Consider the following C function for verifying a user-provided password. Which type of attack it could be vulnerable to? What is a possible input password that could exploit such vulnerability?

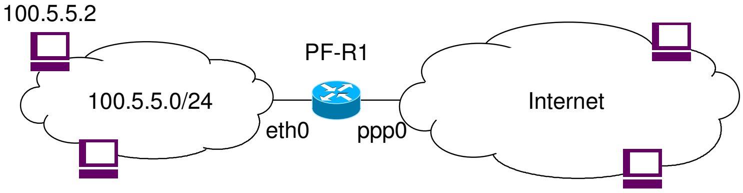
```
int verifyPassword(char* pwd) {
      char str1[8];
      char str2[8];
      strcpy(str1,"SECRET");  // correct password is "SECRET"
      strcpy(str2,pwd);
      if (strncmp(str1,str2,8)==0) return 1; // compares the first 8 characters
      else return 0;
}
```

34) Let us consider the following network scheme, where in the node 100.5.5.2 there is a HTTP web server (TCP port 80) and a SMTP mail server (TCP port 25); you are requested to configure the filtering table of the router R1 so that:

i) from external clients it is possible to access to the internal web server (node 100.5.5.2, TCP port 80);

ii) from internal clients it is possible to access any external web server (port 80);

iii) all client/server and server/client communications between the internal SMTP mail server and possible external SMTP servers are enabled; that is, internal SMTP Client → external SMTP Server (TCP port 25), and external SMTP Client → internal SMTP Server (TCP port 25).



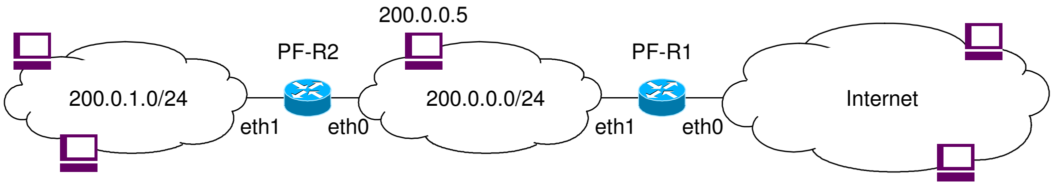
35) Let us consider the following company network formed by an internal network and a DMZ separated by a screening router R2, and connected to the external public network (Internet) through the screening router R1, as shown in figure.
You are requested to configure the filtering table of R1 so that:

a) it is possible to establish application level client→server communications (through any transport protocol) from any DMZ node to any external node;

b) it is blocked any attempt to establish a client→server communication from the external network to the DMZ;

c) it is blocked any communication between the internal and the external networks;

d) it is possible to establish TCP connections from the external network to the node 200.0.0.5 TCP port 80 (HTTP).


200.0.1.0/24
PF-R2
eth1
eth0
200.0.0.5
200.0.0.0/24
PF-R1
eth1
eth0
Internet